REMARKS

Claims 1-28, 30, 31, and 33-41 are pending in this application, all of which have been finally rejected as a result of the January 27, 2005 Office Action. Following entry of the present amendment, claims 1, 9, 20, 25, and 31 will have been amended. In view of the amendments and the Request for Continued Examination (RCE) filed herewith, applicants respectfully submit that this case is in condition for allowance.

Following the January 27, 2005 Final Rejection, applicants submitted an after-final response under 37 C.F.R. § 1.116 on March 28, 2005. In response to the March 28, 2005 paper, the Examiner issued a May 4, 2005 Advisory Action that maintained the rejection of the claims, but for different reasons than had previously been set forth in the January 27, 2005 Final Rejection. In particular, in the Advisory Action, the Examiner did not question the novelty or non-obviousness of the claims; instead the Examiner raised, for the first time, the issue of whether the claims were supported by the specification. In this regard, the Examiner stated as follows:

> Applicant's [sic] arguments filed on March 28, 2005 have been fully considered but they are not persuasive. The Examiner was unable to find support for the Applicant's [sic] arguments with respect to the term "without said cryptographic key being stored in a memory" recited in claims 1, 9, 20, 25, and 31. However, the examiner would reconsider once applicant can clearly show support for the above term in the specification.

[5/4/2005 Advisory Action, p. 2.] (While the Examiner mentions independent claims 1, 9, 20, 25, and 31 as reciting the term "without said cryptographic key being stored in a memory," applicant notes that the various independent claims recite different language and should not be construed as having the same meaning.)

After receiving the Advisory Action, the undersigned initiated a telephone interview with the Examiner on May 16, 2005. Applicant directed the Examiner to page 19 of the specification, which explains that a cryptographic algorithm can apply a cryptographic key without the algorithm having "access" to key 248. The Examiner did not agree that this portion of the specification supports the feature of a key not being stored in a memory accessible to the algorithm, but did agree that the originally-filed specification would support the feature of not requiring "access" to the cryptographic key. Specifically, in an Interview Summary, the Examiner states:

> The Examiner noted that without requiring access to key 248 is not the same as wiothout [sic] cryptographic key being stored required by independent claims. However, agreed that the prior art of record does not teach or fairly suggest the proposeed [sic] limitation "without requiring access to cryptographic key [sic]" which is not yet claimed.

At the telephone interview, the undersigned proposed amending the independent claims to recite that the key is applied without requiring "access" to the key. The Examiner indicated that such an amendment would be supported by page 19 of the application. At that time, applicant also proposed filing an RCE to expedite prosecution. In view of this proposal, and in view of the fact that the amendment had been discussed in the interview, the Examiner indicated that the claim amendments would not result in an immediate final action.

While applicants do not agree that the prior version of the independent claims lacks support in the specification, in the interest of furthering prosecution, applicants have amended independent claims 1, 9, 20, 25, and 31 along the lines discussed with the Examiner. In particular:

- Claim 1 now recites: "a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being accessible to said cryptographic algorithm applied by said first of said plurality of secure repositories".

- Claim 9 now recites: "a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory accessible to said cryptographic algorithm".

- Claim 20 now recites: "a first set of computer-executable instructions which converts encrypted data into decrypted data by applying a cryptographic key to said encrypted data without said cryptographic key being accessible to said first set of computer-executable instructions during the time that said first set of computer-executable instructions applies said cryptographic key".

- Claim 25 now recites: "a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being accessible to said cryptographic algorithm".

- Claim 31 now recites: a "second software process converts encrypted data to decrypted data by using a cryptographic algorithm to apply a cryptographic key to said

encrypted data without said cryptographic key being accessible to said second software process during a time that said second software process is applying said cryptographic key".

Applicants submit that none of the above-quoted features of the independent claims are taught or suggested by the applied references. In particular, the Examiner has previously relied on the Cassagnol reference as teaching claim features related to storage of keys. In the March 28, 2005 paper, applicants explained how Cassagnol protects keys, and we quote that explanation here for the Examiner's convenience:

> Cassagnol is generally directed to cryptography. Principally, Cassagnol describes a system in which cryptographic keys are protected from divulgence by storing them in an EEPROM, securely delivering the keys to a "crypto" module, and physically protecting the EEPROM and the path to the crypto module in order to prevent divulgence of the keys. (Cassagnol, col. 17, ll. 1-15.) The premise of Cassagnol is that the keys can be stored in the EEPROM and transmitted through a channel to the crypto module, because the EEPROM, crypto module, and channel between them are protected so as to prevent the keys from being intercepted. In other words, Cassagnol makes the keys available to the module that will perform cryptographic operations under physically controlled circumstances, but uses various protection means to prevent the keys from being intercepted.

In other words, Cassagnol allows the "crypto" module that applies a key to have access to the key, but stores the key in such a way that prevents the keys from being intercepted by components other than the "crypto' module. As discussed above, claims 1, 9, 20, 25, and 31 recite feature relating to the key being inaccessible to the algorithm (claims 1, 9, and 25), process (claim 31), or instructions (claim 20) that will apply the key. In this regard, claims 1, 9, 20, 25 and 31 are not taught or suggested by Cassagnol. (Applicants also note that the Spies reference was cited in the January 27, 2005 Office Action, but was relied on for a feature that was unrelated to the points discussed in the telephone interview, or to the claim amendments.)

Interview Summary

The undersigned respectfully submits that this paper contains a summary of the substance of the May 16, 2005 telephone interview, as set forth in MPEP 713.04. Since the interview is summarized in this paper, no separate summary of the interview is required.

Conclusion

For the foregoing reasons, the independent claims (1, 9, 20, 25, and 31) are patentable, and the dependent claims (2-8, 10-19, 21-24, 26-28, 30, and 33-41) are patentable at least by reason of their dependency. Thus, applicants respectfully submit that that this case is now in condition for allowance.

Date: July 26, 2005

Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439